InSecTT Newsletter January 2022

Contents

Welcome!

This is the **January 2022 edition** of the InSecTT newsletter, highlighting news & achievements from InSecTT during Q4 2021.

Please distribute this newsletter to all interested parties in your organization. We appreciate your feedback, please send comments or requests to Insectt@v2c2.at.

Enjoy the reading!

New focus session "Intelligent, Secure and Reliable Wireless Systems Focus area overview" at MIKON 2022

Dec 16, 2021

Dependable wireless communication gains its momentum as it is envisioned as a backbone of many interesting applications in various industrial domains. However, to successfully deploy such bring those there seems still some lack of confidence for applying wireless solutions to industrial processes in a wider area. These demanding research challenges will be addressed in a special session co-organized by the European research project InSecTT (Intelligent Secure Trustable Things – https://www.insectt.eu/) that will cover MIKON 2022 conference topics that may be used to bring intelligent, secure, and reliable wireless systems closer to reality.

The submissions may address the following specific topics: AI/ML for wireless transmission, including explainable AI/ML; dependable wireless communication, real-time monitoring, and response; real-time critical communication; verification and validation of reliable wireless communication.

More on MIKON 2022 can be found on https://www.linkedin.com/showcase/microwave-radar-week-mrw2022/ and https://www.linkedin.com/feed/update/urn:li:activity:6872421345695727616/ and

The conference has been postponed to **September 12-14, 2022. The new deadline for paper submission is changed to April 14, 2022**. More details and an updated conference calendar is available on the conference website: https://mrw2022.org/mikon

InSecTT has a second new liaison: InSecTT and DAIS

Dec 15, 2021

The liaison will allow a close collaboration between teams from both projects on creating intelligent, secure, and trustworthy systems. We are for example planning to conduct joint technical workshops and panel discussions to discuss concepts where we can benefit from each other's expertise. We are also planning to explore future opportunities, such as joint activities in standardization events and organizing joint summer school and training events.

InSecTT (https://insectt.eu) started in June 2020 and receives funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876038. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Sweden, Spain, Italy, France, Portugal, Ireland, Finland, Slovenia, Poland, Netherlands, and Turkey. It is coordinated by Michael Karner (Michael.karner@v2c2.at) from Virtual Vehicle.

DAIS (https://dais-project.eu) started in May 2021 and receives funding from the ECSEL Joint Undertaking (JU) under grant agreement No 101007273. The JU receives support from the European Union's Horizon 2020 research and innovation program and Sweden, Spain, Portugal, Belgium, Germany, Slovenia, Czech Republic, Netherlands, Denmark, Norway, and Turkey. It is coordinated by Ali Balador (Ali.balador@ri.se) from RISE.

Open-Kth

Dec 14, 2021

@KTH continues to add capabilities to its AD-EYE testbed. OPEN-KTH is an open Lidar dataset of the KTH campus. Watch a video about it here: https://www.adeye.se/open-kth

For an overview and advancements of the KTH AD-EYE testbed, see here: https://youtu.be/LNjM94oovSM

A new project liaison: InSecTT and ERATOSTHENES

Dec 7, 2021

We are very pleased to announce the newly started liaison of projects InSecTT and ERATOSTHENES !

This liaison will allow a close collaboration of teams from both projects on trustworthiness in (A)IoT. We plan joined technical workshops to discuss requirements and concepts, using each other project's expertise for mutual benefits. In addition, discussions have started to explore future opportunities for joined events, like workshops on conferences and presentations at exploitation events.

Project ERATOSTHENES (eratosthenes-project.eu) started in October 2021 and is funded under H2020-EU.3.7.4. It is coordinated by Konstantinos Loupos (konstantinos.loupos@inlecomsystems.com) from INLECOM.

Project InSecTT (https://www.insectt.eu/) started in June 2020 and receives funding by ECSEL Joint Undertaking (JU). The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Sweden, Spain, Italy, France, Portugal, Ireland, Finland, Slovenia, Poland, Netherlands, Turkey. It is coordinated by Michael Karner (Michael.Karner@v2c2.at) from Virtual Vehicle

KTH: Courses on smart Cyber-Physical Systems (CPS)

Dec 6, 2021

KTH: Courses on smart Cyber-Physical Systems (CPS)

A new course will give @KTH students the basics of one of the hottest technology subjects: smart Cyber-Physical Systems (CPS). The course is a result of collaboration between three departments at KTH and with Ericsson Research and emphasis risk and opportunities of future CPS, systems thinking, and artificial intelligence as deployed in, and with, CPS.

"To be able to invest in new technology, we need people at expert- and management level with knowledge in the area," says @Martin Törngren at KTH, who has been involved in developing the course.

Read more about the new course: https://www.kth.se/indek/nyheter/framtida-ledare-far-koll-pa-cyberfysiska-system-1.1116385

During the fall 2021, KTH also developed a new course on CPS safety and cyber-security. Safety and security are increasingly important for the design of complex technological systems, as they are becoming more intelligent, always connected, and influencing the societal infrastructure at all levels.

"Current education tends to emphasize either safety or cyber-security. This course, on the other hand, gives an overview of both topics and their relationships".

The first instance of the course was given for PhD students and industry. The plan is to make it available in a modified form later for engineering education and distance education.

See more information here: https://www.kth.se/student/kurser/kurs/MF240V?l=en

Following up the Scandinavian Conference on Systems and Software Safety (SCSSS)

Dec 2, 2021

Did you miss out on the 9th edition of the Scandinavian Conference on Systems and Software Safety (SCSSS)? Don't despair! You can read some presentations afterwards, and here is a recap of the popular event:

• @Simon Burton, @Fraunhofer IKS, addressed the safety assurance of automated driving, emphasizing how to deal with machine learning.

• @Sven E. Hammarberg, @BVR Academy & Investigations, talked about the Boeing 737 Max accidents.

• @Fredrik Törner, @Volvo Cars, presented the evolving safety standards landscape for automated driving.

Find the complete program and presentations here: http://safety.addalot.se/2021/program

Thanks to all 130 participants!

The event took place in Gothenburg on November 23–24, and was organized by the two Swedish competence networks, ICES https://www.linkedin.com/company/ices-theindustrynetwork/ at @KTH and @Safer at @Chalmers.

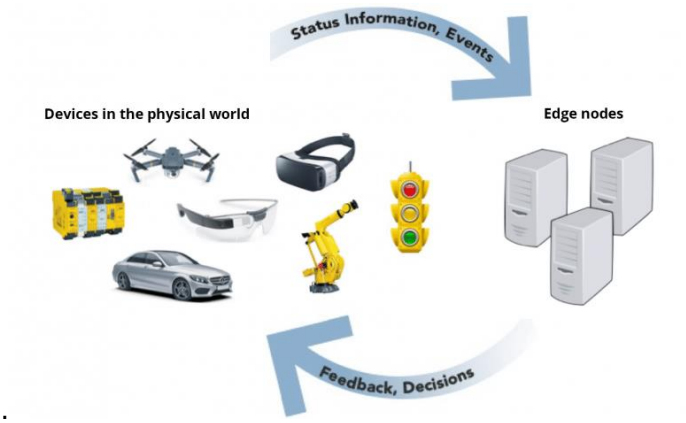
Workshop on Trustworthy edge computing by KTH

Dec 1, 2021

How to assure safety and security in edge computing applications? And how to work with machine learning for these systems while ensuring trustworthiness?

Join a hybrid workshop on December 17.

The workshop is arranged by KTH Royal Institute of Technology and is part of the 6th ACM/IEEE Symposium on Edge Computing (SEC), 2021



InSecTT virtual booth @ EFECS

Nov 23, 2021

Get insights on InSecTT project at the virtual booth during the #EFECS from 23 - 25 November. If you want to know how we work on our vision of bringing AI+IoT together - visit us!

Connected Transportation Solutions

Nov 22, 2021

An example use case of #InSecTT is Intelligent Automation Services for Smart Transportation, with an objective to improve the reliability, safety and security of the systems used in #railway.

#Klas #TRX R6 is the onboard compute gateway underpinning these R&D efforts.

The TRX R6 provides developers with an open architecture, with the flexibility to connect to multiple systems onboard. With #5G available on the TRX R6, researchers are assessing how #IoT and #reliableAI can make use of the next generation of mobile connectivity to deliver on the #InSecTT smart transportation objectives.

Securing Train to NOC Networks

Nov 20, 2021

Successful #IoT implementations in #railway, will rely on data transmissions that are secure and come with zero data loss. Assuring #reliableAI can be evolved based on trusted data from remote train systems. #Klas is collaborating with #InSecTT researchers to develop intelligent routing based on the next generation of #5G mobile connectivity.

By leveraging, Klas compute gateways, developers are implementing #AI based virtual machines that ensure reliable data exchanges, required for the efficient implementation of smart, trustable, safe, and secure systems for rail automation.

InSecTT Consortium Meeting, Madrid, Spain

Nov 15, 2021

The InSecTT consortium meeting started - with several partners joining in person and also online. A great pleasure to meeting so many partners personally but also seeing and hearing you online: we have the best conditions for fruitful discussions! Thanks a lot to our partner Indra for hosting the meeting!

One-way delay measurement without accurate clock synchronization

Nov 11, 2021

Communications delay is one of the most critical metrics for many applications today. Real-time applications demand low and stable delay to work disrupt-free. For example, video monitoring and analysis are a big part of today's industrial operations. For safe and efficient use of video, transferring the content reliably and with low latency is essential, which requires continuous measurement that the latency requirements are met.

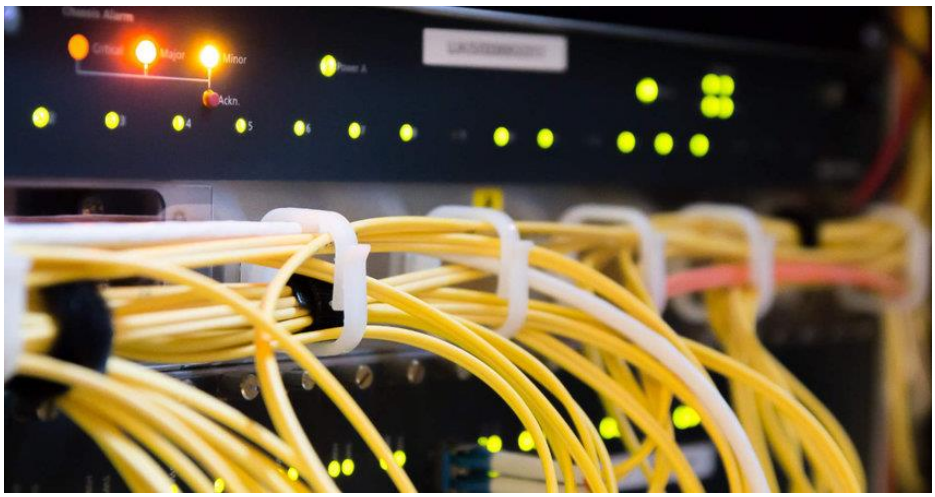
Measuring one-way delays for network traffic necessitates accurate clock synchronization between measurement points. This is sometimes hard to obtain and maintain for different reasons. #Kaitotek, a partner in #InSecTT, has developed an algorithm in the project that detects clock synchronization issues and, in real-time, corrects the measured delay values for application traffic accordingly. The solution is being integrated into their #Qosium, passive QoS/QoE measurement product.

Continuous network quality measurement for securing mission-critical applications

Nov 6, 2021

Traditionally, network quality has been measured periodically with artificial test traffic. However, when increasingly mission-critical applications and services are being used over networks, this measurement does not provide accurate and reliable enough results to determine how well the network performs. #Kaitotek, a partner in #InSecTT, has revolutionized how network performance and quality, like one-way delays, jitters, and loss, is measured and monitored. Instead of burdening networks with test traffic, Kaitotek's #Qosium solution passively measures network quality for real active applications. The measurement can be deployed even to embedded devices, making it possible to obtain even truly end-to-end connection quality monitoring, regardless of the underlying network technologies.

The real-time measurement data provides essential data for control systems and AI mechanisms to adjust networks and applications to cope with the prevailing network conditions. The use cases include, for example, application adaptation, dynamic routing and network resource management, and security monitoring from traffic characteristics.



Towards network quality situation awareness

Nov 3, 2021

Communications networks are the key to the modern industrial environments. Networks serve mission-critical applications that directly reflect business efficiency and operation safety.

#Kaitotek creates rich and real-time visibility for industry about their network quality and how applications experience it. The basis is the continuous network quality measurement that feeds the situation awareness solution with real-time measurement data about network Quality of Service (QoS). This data is processed for KPIs and visualized to quickly see how the network performs in terms of applications used, time, and location.

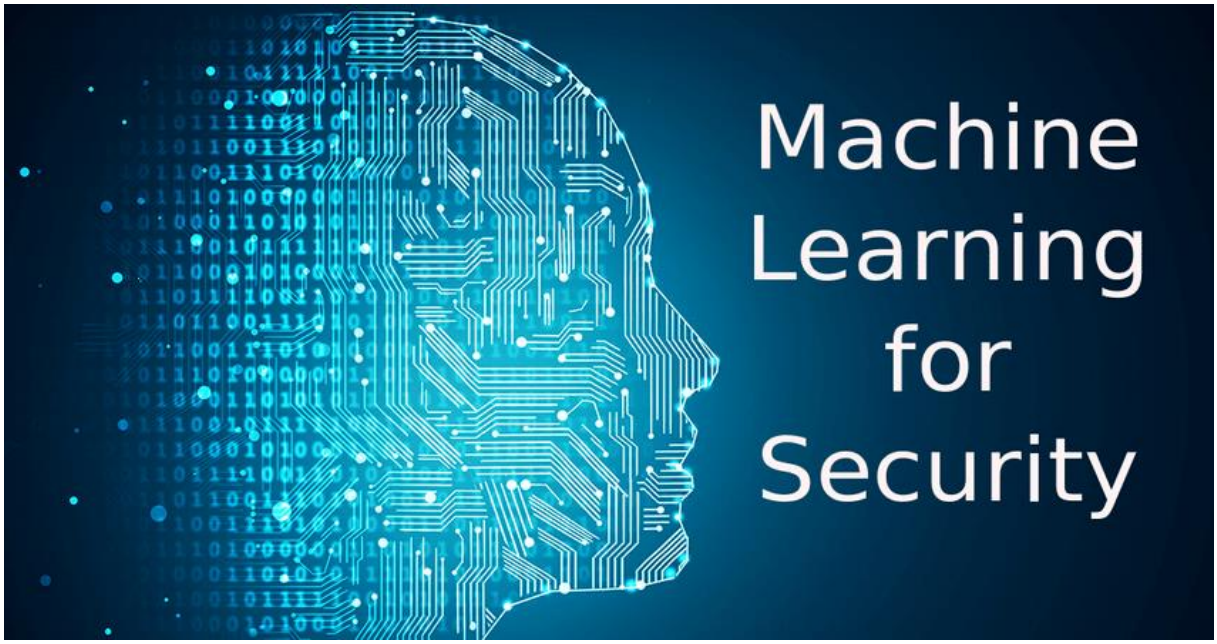
Kaitotek pilots the solution, #Qosium Storage, in the development phase in the Port of Oulu. The measurement is installed on tens of cargo handling vehicles using a private LTE network. A port operator is provided with a solution to detect changes in the port network quality before they harm/disrupt the cargo operations. The heatmap visualization shows where problems are located and which vehicles they affect. Historical data helps analyze how the network performance has evolved and taking SLA reports.

Physical Tamper Attacks Can Be Detected By Machine Learning Methods

Oct 29, 2021

Within the InSecTT project JKU is working on the detection of physical tamper attacks in OFDM-based communication systems with deep learning approaches using physical layer information. We focus on scenarios with static transmitters and receivers while the attacker changes antenna orientation or position of transmitter and/or receiver. Main challenge is to distinguish this attack from environmental changes like the movement of people during regular operation. Deep learning approaches are capable of solving this issue.

We have published first results in this paper(https://ieeexplore.ieee.org/document/9403404) and is working on further improving this method.

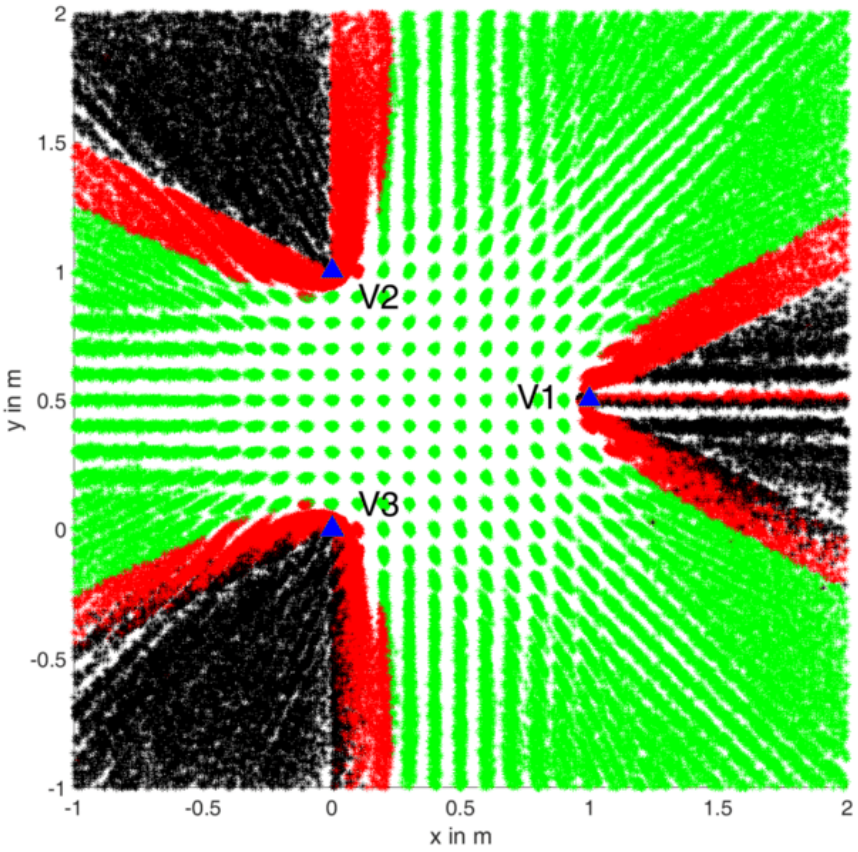


TDOA-Enhanced Distance Bounding Improves Security in Industrial Environments

Oct 21, 2021

Within the InSecTT project JKU is working on enhancing the well-known Distance Bounding protocols by adding passive verifiers that perform TDOA measurements. Distance bounding protocols ensure that a legitimate node, e.g. a wireless car key, is located within a certain distance to a proving entity, e.g. the car. This can improve the security not only for wireless car access but also in industrial environments such as factories. By using our approach, an attacker that could trick the regular distance bounding protocol, would not be able to access restricted factory areas or get access to the car because the TDOA measurements would uncover the attack.

JKU has published a paper on this topic and is working on further developing the TDOA-Enhanced Distance Bounding approach. https://ieeexplore.ieee.org/document/9114460



InSecTT@ International Conference of Computer Vision

Oct 20, 2021

InSecTT project will be present @ ICCV 2021 one of the most important venues worldwide for computer vision research. University of Modena and Reggio Emilia and Technische Universität München will present a joint work about the use of purely synthetic data for training efficient and effective people detection, tracking and ReID systems. Check out ICCV in October and take a look at the paper “MOTSynth: How Can Synthetic Data Help Pedestrian Detection and Tracking?” https://arxiv.org/abs/2108.09518.

Thanks and congrats to all the authors who made it possible Matteo Fabbri, Guillem Braso, Gianluca Maugeri, Orcun Cetintas, Riccardo Gasparini, Aljosa Osep, Simone Calderara, Laura Leal-Taixe, Rita Cucchiara.

InSecTT at the Green Tech Innovators Club

Oct 19, 2021

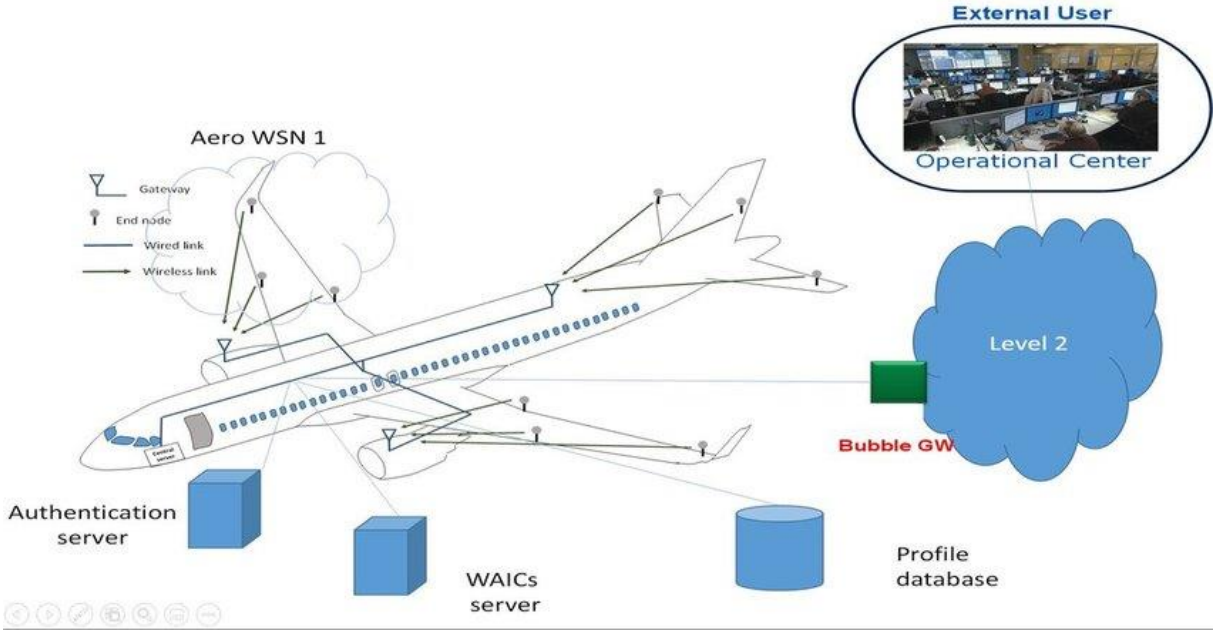
Why is it that human progress often seems to be tied to polluting our environment, damaging fauna and flora? Does it have to be that way? There is a rethinking going on, joining forces to combine human well-being with environmental sustainability. #greentechvally in the south of Graz is a hotspot for innovative energy and environmental technology. So it was logical to join forces and discuss what the #insectt vision working on AI + IOT = AIOT can do for our world. I had to pleasure to present ideas from InSecTT at the Green Tech Innovators Club 12.10.2021. For more information see Das war der Green Tech Innovators Club October 2021

Wireless avionics intra-communications

Oct 14, 2021

ISEP is working on the lower layers of the emerging technology for communications on board aircraft called wireless avionics intra-communications or WAICs. The main objective is the design and improvement of the lower layers, particularly to increase the trust in this technology from the different stakeholders and general users of the aviation industry and in the end to enable the concept of “fly–by-wireless”.

The concept of “fly-by-wireless” will allow future aircraft to be completely modernized by a reliable wireless transmission infrastructure with self-healing, automatic troubleshooting and reconfiguration that will replace many of the low or medium critical cabling subsystems of an aircraft, making it lighter, more flexible and with several advantages such as increased payload, weight reduction, higher fuel efficiency, etc.



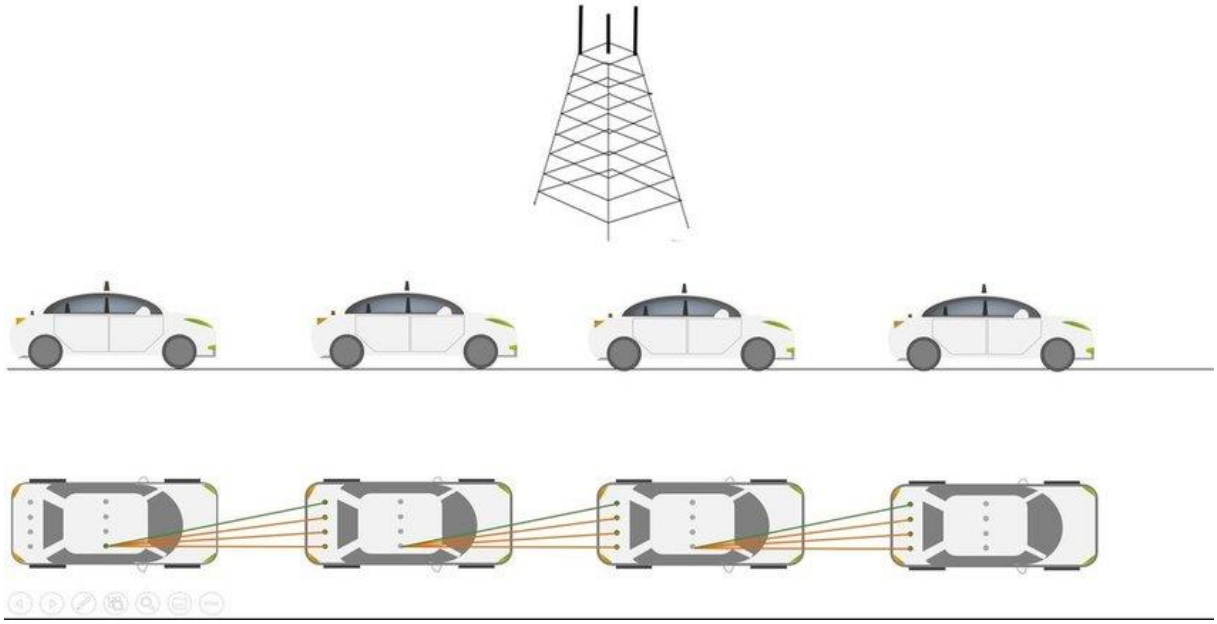
Wireless platooning

Oct 13, 2021

ISEP is one of the contributing partners to the use case of wireless platooning applications. The core of our contribution is on the physical and medium access control technologies

based on multiple antenna systems and artificial intelligence to improve the communications between the elements of a platoon and the roadside infrastructure. The platoon of autonomous or semi-autonomous vehicles aims to be connected to cloud and edge infrastructure. This infrastructure will help, using artificial intelligence and machine learning, with improved decision-making, obstacle/risk detection, route planning and emission reduction of a set of platoons or vehicles in a smart city.

One of the objectives is to improve the experience of drivers, passengers, stakeholders, and also pedestrian users. The main idea is to use a combination of V2V and V2I technologies reducing interference and allocating resources that allow vehicles to communicate reliably and under the minimum latency bounds necessary to reduce potential safety issues. ISEP is developing improved V2V and V2I multiple antenna and propagation models that recreate the diversity found in the platoon scenarios, for example inside tunnels, with reflections and waveguide effects of tall buildings, with obstacles or scatterers and with ground reflections that will make system level simulations more accurate.



Reference architecture

Oct 6, 2021

ISEP is the leader of the task of the reference architecture and reference implementation of the InSecTT project. The reference architecture is a set of guidelines and collection of best

practices to accommodate, design and implement the necessary infrastructure to support dependability, security, trust, and privacy in IoT use cases in different industrial domains. The reference architecture is an evolution of the predecessor architecture of the DEWI and SCOTT projects. This improved architecture targets the impact analysis of the new technology developments such as cloud, edge computing, 5G, multiple interface nodes and mainly artificial intelligence and machine learning on IoT architectures.

The reference architecture is also a collection of expertise and examples of multiple use cases of three different projects towards achieving dependable, secure, trustable, and safe AI-IoT applications for industrial connectivity. The reference architecture consists of multiple views or models that allow designers to analyze the system from multiple perspectives that fit the new requirements of multiple stakeholders. The reference architecture allows us to look at use-cases from a high-level perspective, identifying functionalities, entities, interfaces, communication and processing hardware standards, potential vulnerabilities associated with each interface or functionality, and in many cases, it provides a detailed forensic analysis of building blocks and indicators of stress in different parts of the architecture.

The Insectt architecture is based on the concept of the Bubble, a concept developed in the project DEWI that has been adapted to the new technologies. A bubble is a set of communicating industrial objects and industrial infrastructure encapsulated under a single physical or virtualized cloud gateway infrastructure to ensure security and confined, secured and private communication. The services inside the bubble are enabled by the unique instance of the bubble gateway, guaranteeing the secure access from external sources and protection from malicious attacks, being compatible with modern technologies such as Edge, cloud computing, as well as block chain, and 5G direct cloud connectivity technologies.

The reference architecture also allows us to introduce the concept of security and trustworthiness metrics calculated with different models or approaches across different layers and entities of the architecture. This metrics approach is relevant for future certification and standardization of technologies related to AI and IoT products and services. This has a high impact on the future consumer market and economy of the EU zone. The objective of the task is also to introduce the concept of trust by design in AI-IoT systems.

System level simulation

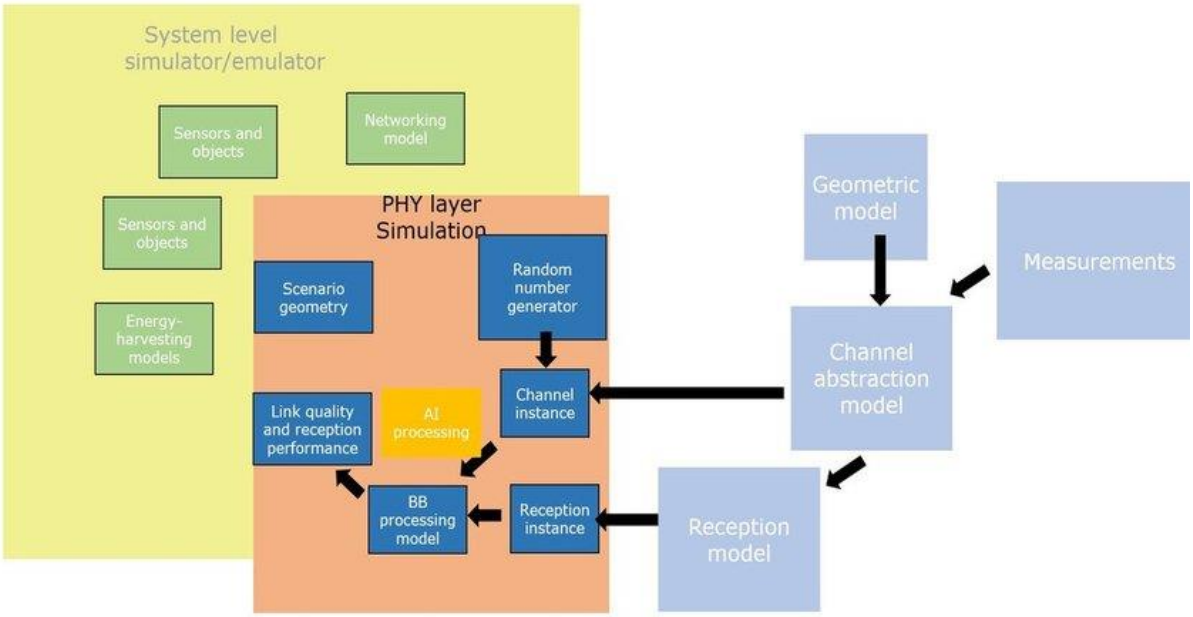
Oct 5, 2021

A crucial aspect in the design, validation and testing of modern IoT use cases is the ability to recreate most of the physical phenomena and networking protocols of the system in software/hardware platforms using realistic models. These software platforms are also called system level simulators. CISTER/ISEP is building a detailed system level simulator for two IoT use cases: wireless platooning and wireless avionics intra-communications.

The objective is to evaluate the detailed performance of the different network elements with an implementation of different reliability and security issues. These issues include detailed

fading distributions, interference, and also cybersecurity attacks and their corresponding countermeasures using artificial intelligence and machine learning algorithms.

The main attacks and issues that are being considered lie in the physical layer such as jamming interference, eavesdropping, man in the middle, node capture, node tapering, denial of service, etc. Upper layer issues and attacks are also considered in a basic form: spoofing, man-in-the-middle, tampering, repudiation, denial of service, etc.



Congratulations - TU Delft startup team ZED gets Dutch takeoff-1 grant

Oct 2, 2021

TU Delft startup Zero Energy Development (ZED, http://zed-iot.com) is a combination of an innovation lab, service provider, and technical and scientific consultancy, that delivers batteryless (and low power) Internet of Things (IoT) solutions that can harvest energy from their surroundings, sense the environment at the same time and wirelessly transmit the sensed information, providing insightful analytics. ZED develops new, sustainable, and scalable energy harvesting (EH-)IoT systems, based on the needs and requirements of clients. Three of the five core members of ZED are from InSecTT project: associate professor Dr. R.R. Venkatesha Prasad, Postdoc Ir. S. Narayana, Ir. N.H. Hokke, and PhD student Ir. S. Sharma, and is guided by Prof. Dr. John Schmitz (co-founder of NXP). ZED wants to be the springboard that can roll out these innovations from the university labs to the

factory floors. By developing high TRL prototypes ZED wants to validate the team's EH innovations not only from a technical but also from a business perspective.

Trustworthy design

Oct 1, 2021

In InSecTT, partner ISEP targets the use of different trustworthiness metrics for wireless systems as well as for artificial intelligence and machine learning algorithms to evaluate the performance of the new convergence between AI and IoT systems. Trustworthiness metrics have been inherited from the project SCOTT using an extension of the ARMOUR security metrics. The objective is to analyze the metrics across different layers and across different entities of the two use cases where ISEP collaborates: Wireless platooning and wireless avionics intra-communications. Trustworthiness metrics are used in the project InSecTT in an attempt to include end user perception of new technologies and increase the trust on the new developments and therefore speed up their adoption.

…